*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**DATE(S) ISSUED:**

12/18/2013

**1/15/2014 - UPDATED**

**SUBJECT:**

Increase in attacks against Web Servers running PHP

**DESCRIPTION:**

Since December 12, 2013, CIS has seen approximately 150 - 200 events per day related to the worm known as Linux.Darlloz. The worm exploits certain versions of PHP that are configured to run as a Common Gateway Interface (CGI) script. The Common Gateway Interface (CGI), defined in RFC3875, is a standard method for web server applications to assign web page generation tasks to executable files. PHP is a server side scripting language used to power websites. Old versions of PHP do not properly handle unexpected queries passed to it when running as a CGI. Symantec published an article in late November (http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices) discussing the usage of CVE-2012-1823 in the worm Linux.Darlloz. The worm is currently targeting multiple CPU architectures (X86, ARM, MIPS, and PPC).

The Linux.Darlloz worm has been spreading via integrated network devices (EX: home routers, small business networking equipment) and web servers running outdated versions of PHP.

**UPDATE:**

**The CIS SOC has seen a continued trend of PHP attacks utilizing vulnerabilities published under CVE-2012-1823. Analysis of the related events has shown several malware campaigns utilizing the vulnerability as an attack vector. In addition to the linux.Darlloz payloads, a large portion of the attacks have been associated with a DDOS botnet. Several custom Linux executables and scripts along with the usage of popular backdoors have also been logged.**

**With the increasing diversity of the these attacks, it is recommended that servers running PHP be evaluated and updated as necessary.**

**RECOMMENDATIONS:**

To mitigate the spread of the worm and verify devices are not vulnerable, the following actions should be taken:

- PHP versions prior to 5.3.13 and 5.4.3 are vulnerable, and should be upgraded to newer versions.
- Verify which PHP package you are using on your web servers. Running a newer version or a version with patches addressing CVE-2012-1823, CVE-2012-2311, CVE-2012-2335, and CVE-2012-2336 will mitigate the vulnerability.
- Verify devices running a web interface or web server do not have PHP configured for php-cgi.
- Verification can be performed by browsing to the device or server and looking for the following files (Replace “EXAMPLE.COM” with your device or server address.)
  - http://EXAMPLE.COM/cgi-bin/php
  - http://EXAMPLE.COM /cgi-bin/php5
  - http://EXAMPLE.COM /cgi-bin/php-cgi
  - http://EXAMPLE.COM /cgi-bin/php.cgi
  - http://EXAMPLE.COM /cgi-bin/php4
- If you can access one of the above files, but can’t verify the PHP version, check for any available updates for that device. Contact the manufacture if no public information on updates are available.
- If not required, block inbound HTTP requests to
  - /cgi-bin/php
  - /cgi-bin/php5
  - /cgi-bin/php-cgi
  - /cgi-bin/php.cgi
  - /cgi-bin/php4

**REFERENCES:**

http://doc.emergingthreats.net/bin/view/Main/2014704 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1823

http://www.deependresearch.org/2013/12/hey-zollard-leave-my-internet-of-things.html?m=1

http://www.exploit-db.com/exploits/29290/

http://www.symantec.com/security_response/writeup.jsp?docid=2013-112710-1612-99

http://msisac.cisecurity.org/advisories/2012/2012-027.cfm